CYBERSECURITY
& Information Systems Digest

The Latest From the Cybersecurity & Information Systems Information Analysis Center // September 21, 2021

SUBMIT A TECHNICAL INQUIRY

Shutterstock

NOTABLE TECHNICAL INQUIRY

How can the smart city concept be applied to military bases, and what security concerns would need to be assessed?

Smart cities' critical infrastructure, economy, and governance are designed to sustainably improve the well-being of residents (U.S. Government Accountability Office [GAO], 2019). Critical infrastructures, such as energy, electricity grids, communications networks, transportation, and water systems, are digitally enhanced to provide smart services to city residents while ensuring security issues are well monitored and effectively addressed (GAO, 2019). **READ MORE**

SNEAK PEEK

UPCOMING WEBINAR:
Network Survivability Assessment Methodology

DATE:
September 22, 2021

TIME:
12:00 PM

PRESENTED BY:
Philip Payne

HOST:
CSIAC

VOICE FROM THE COMMUNITY

Jess Irwin
Technical Staff, Multimission Cyber Security, Raytheon Intelligence & Space

As a technical staff member subject matter expert, Jess provides nearly 50 years of expertise in systems, software, and whole life engineering. As a systems architect, he has supported several of the largest weapons systems platforms, including the F-35 and B-2. His background in mathematics and physics provides insight into subtle issues related to communications and sensor technologies. He has developed operating systems, compilers, and large-scale systems emulations and is an experienced 3-D game developer. He has a foundational patent in distributed trust architecture and collaborated on Trusted Computing Architecture and Intellectual Property Protection techniques. He is an expert in the tools, techniques, and practices of model-based systems engineering using SysML.

BECOME A SUBJECT MATTER EXPERT

DVIDS

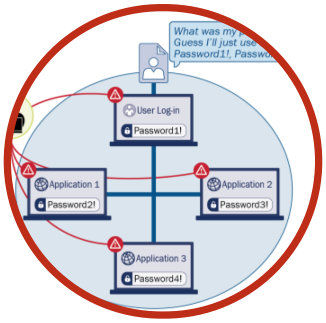
HIGHLIGHT

Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity

Today, President Biden met with private sector and education leaders to discuss the whole-of-nation effort needed to address cybersecurity threats. Recent high-profile cybersecurity incidents demonstrate that both U.S. public and private sector entities increasingly face sophisticated malicious cyber activity. Cybersecurity threats and incidents affect businesses of all sizes, small towns, and cities in every corner of the country, and the pocketbooks of middle-class families. Compounding the challenge, nearly half a million public and private cybersecurity jobs remain unfilled. **LEARN MORE**

FEATURED NEWS

Mobile Application Single Sign-on for First Responders: Final Guide Published



On-demand access to public safety data is critical to ensuring that public safety and first responder (PSFR) personnel can deliver the proper care and support during an emergency. This necessitates heavy reliance on mobile platforms while in the field, which may be used to access sensitive information. However, complex authentication requirements can hinder the process of providing emergency services, and any delay—even seconds—can become a matter of life or death. **READ MORE**

Image: DVIDS

LEARN MORE

Shutterstock

WEBINARS

Network Survivability Assessment Methodology

Presented: *September 22, 2021 12:00 PM - 1:00 PM*
Presenter: *Philip Payne*
Host: *CSIAC*

This presentation describes a network survivability assessment methodology for Cyber-Electromagnetic Activities teams to identify cyber threats early in the acquisition cycle.

The U.S. Department of Defense Acquisition Process begins with a Material Solution Analysis (MSA) and culminates with operations and support. An Analysis of Alternatives (AoA) takes place after all potential solutions are examined to fulfill a need and a preliminary acquisition strategy has been established. The AoA consists of an analytical comparison of the operational effectiveness, suitability, and life-cycle cost of materiel solution alternatives that satisfy the established capability need, as described in an Initial Capabilities Document. Due to the limited amount of system information that is available during the MSA phase for a set of alternatives being considered, a methodology is required to identify potential system threats early in the acquisition cycle.

According to the AoA Handbook from the Office of Aerospace Studies, effectiveness analysis is normally the most complex element of an AoA. The goal of the effectiveness analysis is to determine the military worth of the alternatives being considered when performing mission tasks. The network survivability assessment methodology is applied to provide an assessment of existing security controls effectiveness to protect key mission technologies. **LEARN MORE**

EVENTS

25th Colloquium: Challenges in Teaching Cybersecurity
October 4-6, 2021

(ISC)² 2021 Security Congress
October 18-20, 2021

IEEE Secure Development Conference
October 18-21, 2021

Cybersecurity Symposium for Smart Cities 2021
October 26-27, 2021

I/ITSEC 2021
November 29-December 3, 2021

DoDIIS Worldwide
December 5-8, 2021

MORS Emerging Techniques Forum
December 7-9, 2021

Want your event listed here?
Email contact@csiac.org, to share your event.

- Cybersecurity
- Knowledge Management & Information Sharing
- Modeling & Simulation
- Software Data & Analysis

The inclusion of hyperlinks does not constitute an endorsement by CSIAC or the U.S. Department of Defense (DoD) of the respective sites nor the information, products, or services contained therein. CSIAC is a Defense Technical Information Center (DTIC)-sponsored Information Analysis Center, with policy oversight provided by the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)). Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. government or CSIAC.

4695 Millennium Drive Belcamp, MD 21017
443-360-4600 | info@csiac.org | csiac.org
Unsubscribe | Past Digests

Cybersecurity & Information Systems Information Analysis Center

RECENT NEWS

U.S. Army

Army Lab Gets Green Light for Supercomputing Project

Cybersecurity and Modeling & Simulation

DVIDS

Ransomware Awareness for Holidays and Weekends

Cybersecurity

U.S. Cyber Command

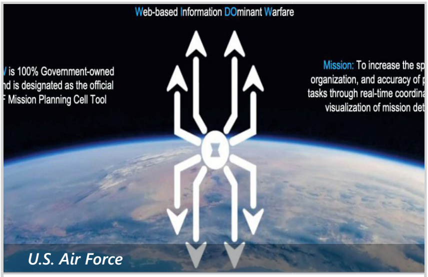
Cyber Command Hosts 2021 Reserve Components Summit

Cybersecurity

RANSOMWARE ATTACK
Your personal files are encrypted
You have 5 days to submit the payment!!!
To retrieve the Private key you need to pay
Your files will be lost
Shutterstock

FBI Alert: "OnePercent" Group Ransomware

Cybersecurity


Web-based Information DOminant Warfare
is 100% Government-owned
nd is designated as the official
Mission Planning Cell Tool
Mission: To increase the sp
organization, and accuracy of
tasks through real-time coordina
visualization of mission det
U.S. Air Force

WIDOW: Nellis AFB Airmen Use Software Tailor-Made for ABMS

Modeling & Simulation and Software Data & Analysis

Shutterstock

Notice of Data Privacy Incident

Cybersecurity